Federal Cyber Service: Scholarship for Service (SFS)

A Federal Cyber Service Training and Education Initiative

Program Solicitation

NSF 01-167

DIRECTORATE FOR EDUCATION AND HUMAN RESOURCES
    DIVISION OF UNDERGRADUATE EDUCATION

LETTER OF INTENT DUE DATE(S) (*optional*): **November 7, 2001**

FULL PROPOSAL DEADLINE(S): December 19, 2001

NATIONAL SCIENCE FOUNDATION

The National Science Foundation promotes and advances scientific progress in the United States by competitively awarding grants and cooperative agreements for research and education in the sciences, mathematics, and engineering.

To get the latest information about program deadlines, to download copies of NSF publications, and to access abstracts of awards, visit the NSF Web Site at:

http://www.nsf.gov

- **Location:**   4201 Wilson Blvd.
  Arlington, VA 22230

- **For General Information (NSF Information Center):**   (703) 292-5111

- **TDD (for the hearing-impaired):**   (703) 292-5090

- **To Order Publications or Forms:**

  Send an e-mail to: pubs@nsf.gov

  or telephone: (301) 947-2722

- **To Locate NSF Employees:**   (703) 292-5111

SUMMARY OF PROGRAM REQUIREMENTS

GENERAL INFORMATION

Program Title: Federal Cyber Service: Scholarship for Service (SFS)

Synopsis of Program:

The Federal Cyber Service: Scholarship for Service (SFS) program seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society. The SFS program is composed of two tracks:

Scholarship Track
The Scholarship Track provides funding to colleges and universities for scholarships in information assurance and computer security fields. These students shall pursue academic programs in information assurance for the final two years of undergraduate study or for two years of master's level study. These students will participate as a cohort during two years of study and activities, including a summer internship in a federal agency at the end of their first year of study. The recipients of the scholarships will become part of the Federal Cyber Service of information technology specialists whose responsibility is to ensure the protection of the United States Government's information infrastructure. Upon graduation after their two-year scholarships, recipients will be required to work for a federal agency for two years as their Federal Cyber Service commitment. The scholarships provide academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students.

Capacity Building Track
The Capacity Building Track provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals via information assurance faculty and program development. Funding for up to $100,000 per year for two years is available.

Partnerships designed to increase participation by underrepresented groups are particularly encouraged. Additional funding of up to $100,000 per year for two years is available to partnerships including Historically Black Universities (HBCUs), Hispanic Serving Institutions (HSIs), and/or Tribal Colleges and Universities (TCUs).

Cognizant Program Officer(s):

- Andrew Bernat, Program Director, Division of Undergraduate Education, telephone: 703.292.4647, e-mail: abernat@nsf.gov.

Applicable Catalog of Federal Domestic Assistance (CFDA) Number(s):

- 47.076 --- Education and Human Resources

ELIGIBILITY INFORMATION

- **Organization Limit:**

  - **Scholarship Track:** The proposing organization must be an accredited U.S. university or college that either (1) has been designated by the National Security Agency as a Center of Excellence in Information Assurance Education (CAE/IAE), or (2) has an information assurance program that meets the criteria equivalent to those necessary for designation as a CAE/IAE. In the latter case, the proposal must demonstrate the program's qualifications for CAE/IAE designation.(See <http://www.nsa.gov/isso/programs/coeiae/measure.htm> for CAE/IAE criteria).

  - **Capacity Building Track:** The proposing organization may be either an accredited U.S. university or college or a consortium. The lead institution in a consortium, must either (1) have a CAE/IAE designation or (2) have an information assurance program that meets criteria equivalent to those necessary for CAE/IAE designation. In the latter case, the proposal must demonstrate the program's qualifications for CAE/IAE designation.(See <http://www.nsa.gov/isso/programs/coeiae/measure.htm> for CAE/IAE criteria).

- **PI Eligibility Limit:** None
- **Limit on Number of Proposals:** None

AWARD INFORMATION

- **Anticipated Type of Award:** Standard or Continuing Grant
- **Estimated Number of Awards:** 5-8 in the Scholarship Track, 3-8 in the Capacity Building Track
- **Anticipated Funding Amount:** $11 million in FY 2002, pending availability of funding

PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

- **Letters of Intent:** Submission of Letters of Intent is optional. Please see the full program announcement/solicitation for further information.
- **Full Proposals:** Supplemental Preparation Guidelines
    - The program announcement/solicitation contains supplements to the standard Grant Proposal Guide (GPG) proposal preparation guidelines. Please see the full program announcement/solicitation for further information.

B. Budgetary Information

- **Cost Sharing Requirements:** Cost Sharing is Specialized. Please see the full program solicitation for further information.
- **Indirect Cost (F&A) Limitations:** No indirect costs may be charged in scholarship track proposals, but proposers may request up to 8 percent of the total budget to address the management and administrative costs associated with operating the SFS scholarship program and may request up to 2 percent of the total budget to address curriculum, laboratory, and faculty development in support of the SFS program. For further information, please refer to the full text of this document. Indirect costs may be charged in Capacity Building Track proposal
- **Other Budgetary Limitations:** Other budgetary limitations apply. Please see the full program announcement/solicitation for further information.

C. Deadline/Target Dates

- **Letters of Intent (*optional*):** November 7, 2001
- **Preliminary Proposals (*optional*):** None
- **Full Proposal Deadline Date(s):** December 19, 2001

D. FastLane Requirements

- **FastLane Submission:** Required

- **FastLane Contact(s):**
    - Antoinette Allen, Computer Specialist, Division of Undergraduate Education, telephone: 703.292.4646, e-mail: duefl@nsf.gov.
    - Fastlane Help Desk, telephone: 800.673.6188, e-mail: fastlane@nsf.gov.

PROPOSAL REVIEW INFORMATION

- **Merit Review Criteria:** National Science Board approved criteria. Additional merit review considerations apply. Please see the full program announcement/solicitation for further information.

AWARD ADMINISTRATION INFORMATION

- **Award Conditions:** Additional award conditions apply. Please see the program announcement/solicitation for further information.
- **Reporting Requirements:** Additional reporting requirements apply. Please see the full program announcement/solicitation for further information.

I. INTRODUCTION

The Federal Cyber Service: Scholarship for Service (SFS) program provides funding to colleges and universities for scholarships and capacity building in the information assurance and computer security fields. A typical scholarship grant will provide four years of funding to enable the institution to cover as many as three cohorts of up to 10, two-year full scholarships (30 two-year scholarships total during the grant period) for study leading to baccalaureate and masters degrees providing technical competence in the area of information assurance and security. A typical capacity building grant will provide funds for institutional and/or faculty development in the area of information assurance and computer security. The program is established by the National Science Foundation (NSF) in accordance with the Federal Cyber Service Training and Education Initiative as described in the President's *National Plan for Information Systems Protection*. This initiative reflects the critical need for Information Technology (IT) professionals specializing in information assurance and security. The expected outcomes of this program include:

- New entrants to the federal workforce with the education and training that will enhance the security of critical federal information infrastructure,

- An increased national capability for the education of IT professionals in critical information infrastructure protection disciplines,

- Increased national research and development capabilities in critical information infrastructure protection, and

- Strengthened partnerships between institutions of higher education and relevant employment sectors.

The scholarship program provides funding for two-year full scholarships for students to pursue academic programs in information assurance for the final two years of undergraduate study or for two years of master's-level study. Upon graduation the recipients of the scholarships will become part of the Federal Cyber Service of information technology specialists whose responsibility is to ensure the protection of the United States Government's information infrastructure. After their two-year scholarships, the recipients will be required to work for a federal agency for two years as their Federal Cyber Service commitment.

The capacity building component of the SFS program provides funds to colleges and universities to improve the quality and increase the production of information assurance and computer security professionals via information assurance faculty and program development.

II. PROGRAM DESCRIPTION

The primary objective of the SFS program is to build information assurance capacity and to provide an educated cadre of information technology professionals who can help assure the protection of the United States Government information infrastructure. The two tracks in this program are described below.

In order to increase information security expertise and capacity at institutions serving underrepresented populations, application by and partnerships with Historically Black Colleges and Universities (HBCUs), Hispanic Serving Institutions (HSIs), and Tribal Colleges and Universities (TCUs) are encouraged.

Scholarship Track:

The SFS program provides funds to colleges and universities for student scholarships in support of education in information technology areas relevant to information assurance and computer security. In return for their scholarship and stipend, students must agree to work after graduation for two years as an information assurance specialist in the Federal Cyber Service for a federal agency.

During the scholarship period, the students will participate in internships at federal agencies and participate in other SFS activities such as conferences, workshops, and seminars. These activities are aimed at developing a community of practice that will enhance their individual and collective skills in an area increasingly important to the health and safety of the United States. The Office of Personal Management (OPM) will partner with the NSF in this program by providing the internships at federal agencies and federal agency placement after graduation. The OPM will also be responsible for the coordination of students as Federal employees, for ensuring that contractual obligations are met by the students during their scholarship period and after graduation, and for assessing whether the program helps meet the personnel needs of the federal government for information infrastructure protection.

Grantee institutions will provide scholarship support to students who compete successfully in a selection process developed by the institution, who meet the SFS eligibility criteria, and who are selected as qualified for employment in the Federal Cyber Service by OPM. It is expected that scholarship participants will receive their degree (undergraduate or master's) within two years of the beginning of their scholarships. Each proposing institution must provide a description of its selection criteria and process, and explain and justify the proposed distribution of scholarship recipients. In particular, institutions must ensure that groups underrepresented in information technology have fair access to scholarships.

To be eligible for consideration for an SFS scholarship, a student must be

- a United States citizen and
- a full-time student within two years of graduation in a coherent formal program that is focused on computer security or information assurance at an awardee institution.

Students identified by their institutions for scholarships must meet selection criteria for federal employment. In addition, internship placements and final job placements may require security clearances. Scholarship recipients may be required to undergo the background investigation required to obtain such clearances.

The selection process for scholarship recipients should include indicators of academic merit and other indicators of future professional success. Multiple indicators may be appropriate in gauging both academic merit (e.g., grade point average, class rank) and professionalism (e.g., motivation, ability to manage time and resources, communication skills). Selection criteria should be flexible enough to accommodate applicants who have diverse backgrounds and with diverse career goals. Federal Cyber Service scholars must continue to demonstrate their eligibility in each semester/quarter of SFS support.

Awardee institutions must submit their lists of candidates for SFS scholarships to OPM for final eligibility approval. OPM will manage the scholars' internships and job placements. OPM will also manage compliance with the mandatory employment component of this program.

It is expected that grantee institutions will provide the infrastructure to recruit and support students, so that a sufficient number of scholarship recipients will graduate. Such an infrastructure might include, for example:

- Recruitment of students, with special consideration to groups underrepresented in SFS fields (i.e., women, racial and ethnic minorities, and persons with disabilities).
- Academic support and mentoring to support students in making progress toward the degree and to prepare students for the workplace.
- Application-oriented experiences to increase the students' understanding of information assurance needs and their relationship to educational preparation and to build their leadership skills.
- Mechanisms to ensure retention of scholarship recipients to degree.

Grantee institutions are also expected to have clearly articulated management and administrative plans for the following program elements. These items must be clearly detailed in the Budget Justification section of the proposal.

- Verification of scholarship candidates' eligibility, including the recipients' academic merit, appropriate affective skills, and enrollment in a designated or equivalent information assurance program.

- Provision of scholarship amounts to be used for expenses normally incurred by full-time students in the institution, including tuition, room and board, and equipment. These shall be included in participant support costs.
- Provision of academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students. These charges shall be included in participant support costs.
- Provision for coordination with OPM for summer intern placements for each student. Students are expected to take Federal intern positions in the summer between their first and second year of scholarship study. The payments for summer internships will take place outside the university grant structure and are not to be included in the budget.
- Provisions for tracking the academic progress of students to determine their continued eligibility throughout the academic part of the program. Subsequent tracking of students to verify that they meet the service obligation will be done by OPM.
- Evaluation of program outcomes.
- Demonstration of ability to partner with the OPM in student hiring and agency placement.

No indirect costs may be charged in Scholarship Track proposals, but proposers may request up to 8 percent of the total budget to address the management and administrative costs associated with operating the SFS scholarship program and institutions may also request up to 2 percent of the total budget to address curriculum, laboratory, and faculty development in support of the SFS program. Funds requested for management and administrative costs, as well as for curriculum, laboratory, and faculty development, must be included in standard budget categories in the proposal budget, and appropriate justification must be provided in the Budget Justification.

Collaborations with industry, non-profit, or state organizations are strongly encouraged to allow students not chosen for the scholarships to participate in student internships and in Federal Cyber Service activities.

The Principal Investigator (PI) will have overall responsibility for the administration of the institution's award, the management of the project, and interactions with NSF and OPM. The PI and the grantee institution are expected to have or to develop an administrative structure that enables faculty, academic administrators, scholarship recipients, and others involved in the project to interact productively during the award period. The PI is expected to be an integral participant in the educational activities of the SFS project. The management plan will be an integral part of the proposal evaluation.

Within the grantee institution, the departments making up the Center of Academic Excellence in Information Assurance Education or equivalent are expected to collaborate in implementing the project plan. To broaden the support of their activities, proposers are encouraged to establish collaborative arrangements with other organizations.

A proposing institution must have a strong program of activity in information assurance with Center of Academic Excellence in Information Assurance Education (CAE/IAE) designation, or must be able to demonstrate that its programs meet criteria equivalent to those necessary for designation as a CAE/IAE by the National Security Agency. Additionally, the institution must demonstrate its continuing commitment to both faculty development and curriculum excellence in information assurance. Proposals should contain documentation of CAE/IAE designation or demonstrate how the program meets the criteria published by the National Security Agency at <http://www.nsa.gov/isso/programs/coeiae/measure.htm>.

Proposals should clearly describe the activities to be undertaken, the processes through which the program elements will be implemented, and plans for documentation. Proposals should also clearly describe the student support structure, plans to manage and administer the program, and evidence of the quality of the institution's educational program in information assurance.

Capacity Building Track:

The SFS program provides for capacity building in information assurance and computer security fields by providing funds to support faculty, institutional and partnership development.

The intent of the Capacity Building Track is to increase the production of high quality information assurance and computer security professionals by providing support for efforts within the higher education system. These efforts may take many forms, but must be designed to

- Increase national capability for the high-quality education of information technology professionals in critical information infrastructure protection disciplines, or
- Strengthen partnerships between institutions of higher education, government, and relevant employment sectors leading to improved educational opportunities in information assurance studies.

Funding for up to $100,000 per year for two years is available. Additional funding of up to $100,000 per year for two years is available for partnerships including minority-serving institutions HBCUs, HSIs, and TCUs.

Indirect costs may be charged against all costs except participant support and equipment.

Typical projects include, but are not limited to, the following:

- *Adaptation and Implementation*: The program wishes to foster collaboration and dialogue among institutions offering courses and programs in information assurance. Consequently, the SFS program supports proposals for the adaptation and implementation of exemplary educational materials, courses, and curricula

that have been developed at CAE/IAE or comparable institutions to promote increased educational capacity in information assurance and computer security education programs.

- *Curriculum and Educational Materials Development*: Supported activities should affect the learning environment, course content, and the experience of instruction. Projects often result in textbooks, laboratory experiments and manuals, software, CD-ROMS, videos, and other courseware. Such products are expected to be widely disseminated through commercial publishers, conferences, workshops, electronic networks, journal articles, and other means. A project's focus may range from the substantial revision of existing instructional materials to the creation of entirely new ones; from a few modules at a single educational level to comprehensive curriculum for multiple years; and from a single subject to the integration of several disciplines.

- *Faculty Development*: Grants are made to CAE/IAE designated or equivalent institutions for the development and implementation of activities that assist faculty from other institutions to learn about recent advances in information assurance and computer security and to improve their instructional capability in these areas. Such activities might include residencies, conferences, workshops, intensive seminars, distance learning opportunities, or a combination of these to bring about the desired professional development for faculty. These activities typically last from a few days to several weeks and are usually conducted in the summer, with follow-up activities during the academic year. To effect long-term change, projects for faculty development should normally span at least two academic years.

  Proposals must describe how faculty participants will be recruited, what level of support will be provided for participants, what evaluation procedures will be used, and what type of follow-up will be provided as participants implement new courses and curricula in information assurance and computer security. Proposals must also describe how institutional teams of two or more members will be formed, and provide evidence of the institutional support that assures that these teams can continue to work towards building institutional capacity once the teams complete their faculty development activities.

  Inclusion of faculty belonging to underrepresented populations and from institutions serving underrepresented populations in such partnerships is strongly encouraged.

- *Technical Experiences*: Well-designed technical experiences in the classroom and in a work environment can give students and faculty a broad, up-to-date, real-world perspective on the information assurance fields. Such experiences typically allow participants to get hands-on exposure to the field and thereby gain confidence in their abilities in technical areas; interact closely with computer security experts; obtain information about various careers available in information

assurance and computer security; become aware of academic preparation necessary for such careers; become acquainted with the environments of other academic institutions, private industry, and government agencies; and develop leadership skills.

Projects providing technical experiences may consist of any combination of activities involving instruction, problem solving, research, deployment of security solutions, and industrial internships. Proposals should describe recruitment strategies, criteria for selection of participants, and the relevance of the planned experiences to the goal of developing expertise in information assurance and computer security.

- *Laboratory Development*: Laboratory or field experiences using suitable modern instrumentation are crucial elements in advanced technology fields. The SFS program supports the development of innovative methods for using laboratory and field exercises to improve students' understanding of basic principles. It also supports use by faculty of modern instrumentation, new technologies, or applications of instruments that extend their instructional capability. The program also encourages the establishment of equipment-sharing arrangements through consortia of institutions developing capacity in information assurance and computer security.

- *Partnerships*: Partnerships between CAE/IAE and equivalent institutions and institutions seeking to enhance their IA programs are strongly encouraged. Such partnerships serve to increase the capacity of the educational system to produce high quality information assurance and security degree recipients. Including private companies and local, state and federal governmental agencies greatly increases the value of such partnerships.

   Inclusion of institutions serving underrepresented populations in such partnerships is strongly encouraged.

Proposals must clearly explain how their project will address the previously stated objectives of the program.

Proposals must describe impact on the production of qualified students, plans to evaluate the success of the project and plans to provide effective dissemination of results.

III. ELIGIBILITY INFORMATION

For the Scholarship Track, the proposing organization must be an accredited U.S. university or college that either (1) has been designated by the National Security Agency as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) or (2) has an information assurance program that meets criteria equivalent to those necessary for designation as a CAE/IAE. In the latter case, the proposal must demonstrate the program's qualifications for CAE/IAE designation. For the Capacity Building Track,

the proposing organization may be either an accredited U.S. university or college or a consortium. The lead institution in a proposing consortium must either (1) have a CAE/IAE designation or (2) have an information assurance program that meets criteria equivalent to those necessary for CAE/IAE designation. In the latter case, the proposal must demonstrate the program's qualifications for CAE/IAE designation. (See <http://www.nsa.gov/isso/programs/coeiae/measure.htm> for CAE/IAE criteria).

An organization may submit no more than one proposal per track per round of competition.

IV. AWARD INFORMATION

The SFS Scholarship Track supports a university- or college-based scholarship program that supports two years of tuition, room and board, and stipend for students in the general area of information assurance and security. The program contains an internship component intended to support hands-on training in the Federal Government that is supported through the award for the internships and other training. A typical award might be approximately $2.5 million for four years supporting three cohort classes of 10 first-year students (year 1), 10 first-year and 10 second-year students (year 2), 10 first-year and 10 second-year students (year 3), and 10 second-year students (year 4). The total award sizes will depend upon the tuition and room and board costs and on the cost of management and development.

The SFS Capacity Building Track supports a university or college or partnership in efforts to increase the numbers of highly qualified degree graduates with emphasis in information assurance and/or computer security. Awards provide up to $100,000 per year for up to two years. Additional funding of up to $100,000 per year for two years is available for partnerships including Historically Black Colleges and Universities (HBCUs), Hispanic Serving Institutions (HSIs) and/or Tribal Colleges and Universities(TCUs).

V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

Letters of Intent: A letter of intent to submit a proposal is requested (but not required) to assist NSF in planning for review. The letter of intent is not a preliminary proposal. It should be a brief statement that lists the submitting organization and any partners, and the intended track (Scholarship or Capacity Building), for the proposal. Letters of intent should be sent by electronic mail to <sfs@nsf.gov> no later than November 7, 2001.

Full Proposal:

Proposals submitted in response to this program announcement/solicitation should be prepared and submitted in accordance with the general guidelines contained in the NSF *Grant Proposal Guide* (GPG). The complete text of the GPG is available electronically on the NSF Web Site at: http://www.nsf.gov/cgi-bin/getpub?gpg. Paper copies of the GPG may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from pubs@nsf.gov.

A Project Data Form must be submitted (via Fastlane) as part of all proposals. The information on this is used to direct proposals to appropriate reviewers and to determine the characteristics of projects supported by the Division of Undergraduate Education. In Fastlane, this form will show up in the list of forms for your proposal only after you have selected the Program Announcement/ Solicitation No. on the Cover Sheet.

A Budget Justification of up to three pages must accompany the budget forms and provide details about line items. Proposals that involve subawards should include a Budget Justification of up to three pages for each subawardees organization.

Organizations intending to submit simultaneous Collaborative Proposals must carefully follow the instructions for electronic submission specified in GPG, Chapter II, Section C.11.b.ii. The titles of the related proposals must be identical and must begin with the words Collaborative Project, and the c ombined budgets of the related proposals should conform to the anticipated individuals award sizes specified in Section IV (AWARD INFORMATION) above. These simultaneous Collaborative Proposals will be treated as a single proposal (with a single Project Summary, Project Description, and References Cited) during the review process.

Proposers are reminded to identify the program solicitation number (NSF 01-167) in the program announcement/solicitation block on the proposal Cover Sheet (NSF Form 1207). Compliance with this requirement is critical to determining the relevant proposal processing guidelines. Failure to submit this information may delay processing.

B. Budgetary Information

Funds requested for equipment and other technology (including, but not limited to, computers, computer-related hardware, software, laboratory or field instrumentation, and scientific or industrial machinery) must be matched by non-Federal funds, equipment, or other technology with a value equal to the funds requested from NSF.

The proposed cost sharing must be shown on Line M on the proposal budget. Documentation of the availability of cost sharing must be included in the proposal. Only items which would be allowable under the applicable cost principles, if charged to the project, may be included as the awardee's contribution to cost sharing. Contributions may be made from any non-Federal source, including non-Federal grants or contracts, and may be cash or in-kind (see OMB Circular A-110, Section 23). It should be noted that

contributions counted as cost-sharing toward projects of another Federal agency may not be counted towards meeting the specific cost-sharing requirements of the NSF award. All cost-sharing amounts are subject to audit. Failure to provide the level of cost-sharing reflected in the approved award budget may result in termination of the NSF award, disallowance of award costs and/or refund of award funds to NSF.

Indirect Cost (F&A) Limitations: No indirect costs may be charged in scholarship track proposals, but proposers may request up to 8 percent of the total budget to address the management and administrative costs associated with operating the SFS scholarship program and may request up to 2 percent of the total budget to address curriculum, laboratory, and faculty development in support of the SFS program. For further information, please refer to the full text of this document. Indirect costs may be charged in Capacity Building Track proposal

Other Budgetary Limitations: The Scholarship Track provides academic year stipends of $8,000 per year for undergraduate students and $12,000 per year for graduate students. The Capacity Building Track provides funding for up to $100,000 per year for two years; additional funding of up to $100,000 per year for two years is available to support the inclusion of HBCUs, MSIs, and TCUs. Funds requested for equipment or other technology may not exceed $100,000 or 10 percent of the total NSF funding request, whichever is larger.

C. Deadline/Target Dates

Proposals must be submitted by the following date(s):

Letters of Intent (*optional*): November 7, 2001
Full Proposals *by 5:00 PM local time*: December 19, 2001

D. FastLane Requirements

Proposers are required to prepare and submit all proposals for this Program Solicitation through the FastLane system. Detailed instructions for proposal preparation and submission via FastLane are available at: http://www.fastlane.nsf.gov/a1/newstan.htm. For FastLane user support, call 1-800-673-6188 or e-mail fastlane@nsf.gov.

Submission of Signed Cover Sheets. The Authorized Organizational Representative (AOR) must electronically sign the proposal Cover Sheet to submit the required proposal certifications (see Chapter II, Section C of the Grant Proposal Guide for a listing of the certifications). The AOR must provide the required certifications within five working days following the electronic submission of the proposal. Further instructions regarding this process are available on the FastLane website at: http://www.fastlane.nsf.gov.

VI. PROPOSAL REVIEW INFORMATION

A. NSF Proposal Review Process

Reviews of proposals submitted to NSF are solicited from peers with expertise in the substantive area of the proposed research or education project. These reviewers are selected by Program Officers charged with the oversight of the review process. NSF invites the proposer to suggest at the time of submission, the names of appropriate or inappropriate reviewers. Care is taken to ensure that reviewers have no conflicts with the proposer. Special efforts are made to recruit reviewers from non-academic institutions, minority-serving institutions, or adjacent disciplines to that principally addressed in the proposal.

Proposals will be reviewed against the following general review criteria established by the National Science Board. Following each criterion are potential considerations that the reviewer may employ in the evaluation. These are suggestions and not all will apply to any given proposal. Each reviewer will be asked to address only those that are relevant to the proposal and for which he/she is qualified to make judgements.

> **What is the intellectual merit of the proposed activity?**
> How important is the proposed activity to advancing knowledge and understanding within its own field or across different fields? How well qualified is the proposer (individual or team) to conduct the project? (If appropriate, the reviewer will comment on the quality of the prior work.) To what extent does the proposed activity suggest and explore creative and original concepts? How well conceived and organized is the proposed activity? Is there sufficient access to resources?
> **What are the broader impacts of the proposed activity?**
> How well does the activity advance discovery and understanding while promoting teaching, training, and learning? How well does the proposed activity broaden the participation of underrepresented groups (e.g., gender, ethnicity, disability, geographic, etc.)? To what extent will it enhance the infrastructure for research and education, such as facilities, instrumentation, networks, and partnerships? Will the results be disseminated broadly to enhance scientific and technological understanding? What may be the benefits of the proposed activity to society?

Principal Investigators should address the following elements in their proposal to provide reviewers with the information necessary to respond fully to both of the above-described NSF merit review criteria. NSF staff will give these elements careful consideration in making funding decisions.

> *Integration of Research and Education*
> One of the principal strategies in support of NSF's goals is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions provide abundant opportunities where individuals may concurrently assume responsibilities as

researchers, educators, and students and where all can engage in joint efforts that infuse education with the excitement of discovery and enrich research through the diversity of learning perspectives.

Integrating Diversity into NSF Programs, Projects, and Activities
Broadening opportunities and enabling the participation of all citizens -- women and men, underrepresented minorities, and persons with disabilities -- is essential to the health and vitality of science and engineering. NSF is committed to this principle of diversity and deems it central to the programs, projects, and activities it considers and supports.

Additional Review Criteria

Reviewers will be asked to consider the merit review criteria with emphasis placed on the SFS program components (see "Program Description"). These include:

- o The quality and completeness of the management and administrative plan. The plan must address all elements expressed in the program solicitation,
- o Designation as a Center of Academic Excellence in Information Assurance Education or approved equivalent programs (Scholarship Track and Capacity Building Track if relevant),
- o Quality of education and research in information assurance at the institution and the extent to which education and research are integrated,
- o Application-oriented experiences to increase the student's understanding of information assurance needs and their relationship to educational practices, with particular emphasis on K-12 education, governmental and industrial partnerships and outreach,
- o Faculty members with specific expertise in information assurance and security as well as professional development for other faculty,
- o Discipline faculty members integrally involved with the scholarship students and working with the students as a cohort, and
- o For the scholarship track, the review may also consider the provision for appropriate student support infrastructure for the successful graduation of scholarship recipients as expressed in the program announcement.

A summary rating and accompanying narrative will be completed and signed by each reviewer. In all cases, reviews are treated as confidential documents. Verbatim copies of reviews, excluding the names of the reviewers, are sent to the Principal Investigator/Project Director by the Program Director. In addition, the proposer will receive an explanation of the decision to award or decline funding.

B. Review Protocol and Associated Customer Service Standard

All proposals are carefully reviewed by at least three other persons outside NSF who are experts in the particular field represented by the proposal. Proposals submitted in response to this announcement/solicitation will be reviewed by Panel Review.

Reviewers will be asked to formulate a recommendation to either support or decline each proposal. The Program Officer assigned to manage the proposal's review will consider the advice of reviewers and will formulate a recommendation.

NSF is striving to be able to tell applicants whether their proposals have been declined or recommended for funding within six months for 70 percent of proposals. The time interval begins on the date of receipt. The interval ends when the Division Director accepts the Program Officer's recommendation.

In all cases, after programmatic approval has been obtained, the proposals recommended for funding will be forwarded to the Division of Grants and Agreements for review of business, financial, and policy implications and the processing and issuance of a grant or other agreement. Proposers are cautioned that only a Grants and Agreements Officer may make commitments, obligations or awards on behalf of NSF or authorize the expenditure of funds. No commitment on the part of NSF should be inferred from technical or budgetary discussions with a NSF Program Officer. A Principal Investigator or organization that makes financial or personnel commitments in the absence of a grant or cooperative agreement signed by the NSF Grants and Agreements Officer does so at its own risk.

VII. AWARD ADMINISTRATION INFORMATION

A. Notification of the Award

Notification of the award is made to *the submitting organization* by a Grants Officer in the Division of Grants and Agreements. Organizations whose proposals are declined will be advised as promptly as possible by the cognizant NSF Program Division administering the program. Verbatim copies of reviews, not including the identity of the reviewer, will be provided automatically to the Principal Investigator. (See section VI.A. for additional information on the review process.)

B. Award Conditions

An NSF award consists of: (1) the award letter, which includes any special provisions applicable to the award and any numbered amendments thereto; (2) the budget, which indicates the amounts, by categories of expense, on which NSF has based its support (or otherwise communicates any specific approvals or disapprovals of proposed expenditures); (3) the proposal referenced in the award letter; (4) the applicable award conditions, such as Grant General Conditions (NSF-GC-1)* or Federal Demonstration Partnership (FDP) Terms and Conditions * and (5) any announcement or other NSF issuance that may be incorporated by reference in the award letter. Cooperative agreement awards also are administered in accordance with NSF Cooperative Agreement Terms and Conditions (CA-1). Electronic mail notification is the preferred way to transmit NSF awards to organizations that have electronic mail capabilities and have requested such notification from the Division of Grants and Agreements.

*These documents may be accessed electronically on NSF's Web site at http://www.nsf.gov/home/grants/grants_gac.htm. Paper copies may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from pubs@nsf.gov.

More comprehensive information on NSF Award Conditions is contained in the NSF *Grant Policy Manual* (GPM) Chapter II, available electronically on the NSF Web site at http://www.nsf.gov/cgi-bin/getpub?gpm. The GPM is also for sale through the Superintendent of Documents, Government Printing Office (GPO), Washington, DC 20402. The telephone number at GPO for subscription information is (202) 512-1800. The GPM may be ordered through the GPO Web site at http://www.gpo.gov.

Special Award Conditions

C. Reporting Requirements

For all multi-year grants (including both standard and continuing grants), the PI must submit an annual project report to the cognizant Program Officer at least 90 days before the end of the current budget period.

Within 90 days after the expiration of an award, the PI also is required to submit a final project report. Approximately 30 days before expiration, NSF will send a notice to remind the PI of the requirement to file the final project report. Failure to provide final technical reports delays NSF review and processing of pending proposals for that PI. PIs should examine the formats of the required reports in advance to assure availability of required data.

NSF has implemented an electronic project reporting system, available through FastLane. This system permits electronic submission and updating of project reports, including information on project participants (individual and organizational), activities and findings, publications, and other specific products and contributions. PIs will not be required to re-enter information previously provided, either with a proposal or in earlier updates using the electronic system.

VIII. CONTACTS FOR ADDITIONAL INFORMATION

General inquiries regarding Federal Cyber Service: Scholarship for Service should be made to:

- Andrew Bernat, Program Director, Division of Undergraduate Education, telephone: 703.292.4647, e-mail: abernat@nsf.gov.

For questions related to the use of FastLane, contact:

- Antoinette Allen, Computer Specialist, Division of Undergraduate Education, telephone: 703.292.4646, e-mail: duefl@nsf.gov.

- Fastlane Help Desk, telephone: 800.673.6188, e-mail: fastlane@nsf.gov.

IX. OTHER PROGRAMS OF INTEREST

The NSF *Guide to Programs* is a compilation of funding for research and education in science, mathematics, and engineering. The NSF *Guide to Programs* is available electronically at http://www.nsf.gov/cgi-bin/getpub?gp. General descriptions of NSF programs, research areas, and eligibility information for proposal submission are provided in each chapter.

Many NSF programs offer announcements or solicitations concerning specific proposal requirements. To obtain additional information about these requirements, contact the appropriate NSF program offices. Any changes in NSF's fiscal year programs occurring after press time for the *Guide to Programs* will be announced in the NSF E-Bulletin, which is updated daily on the NSF web site at http://www.nsf.gov/home/ebulletin, and in individual program announcements/solicitations. Subscribers can also sign up for NSF's Custom News Service (http://www.nsf.gov/home/cns/start.htm) to be notified of new funding opportunities that become available.

Information about the Computer Science, Engineering, and Mathematics Scholarships (CSEMS) program, which provides additional student funding, is available at <http://www.ehr.nsf.gov/EHR/DUE/programs/csems/>.

ABOUT THE NATIONAL SCIENCE FOUNDATION

The National Science Foundation (NSF) funds research and education in most fields of science and engineering. Awardees are wholly responsible for conducting their project activities and preparing the results for publication. Thus, the Foundation does not assume responsibility for such findings or their interpretation.

NSF welcomes proposals from all qualified scientists, engineers and educators. The Foundation strongly encourages women, minorities and persons with disabilities to compete fully in its programs. In accordance with Federal statutes, regulations and NSF policies, no person on grounds of race, color, age, sex, national origin or disability shall be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving financial assistance from NSF (unless otherwise specified in the eligibility requirements for a particular program).

Facilitation Awards for Scientists and Engineers with Disabilities (FASED) provide funding for special assistance or equipment to enable persons with disabilities (investigators and other staff, including student research assistants) to work on NSF-supported projects. See the program announcement/solicitation for further information.

The National Science Foundation has Telephonic Device for the Deaf (TDD) and Federal Information Relay Service (FIRS) capabilities that enable individuals with hearing impairments to communicate with the Foundation about NSF programs, employment or general information. TDD may be accessed at (703) 292-5090, FIRS at 1-800-877-8339.

The National Science Foundation is committed to making all of the information we publish easy to understand. If you have a suggestion about how to improve the clarity of this document or other NSF-published materials, please contact us at plainlanguage@nsf.gov.